

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | | |
|--|---|--------------------------------|
| -----X | : | |
| CBF INDUSTRIA DE GUSA S/A, <i>et al.</i> , | : | |
| | : | |
| Plaintiffs, | : | |
| | : | <u>MEMORANDUM ORDER</u> |
| -against- | : | |
| | : | 13-CV-2581 (PKC) (JLC) |
| AMCI HOLDINGS, INC., <i>et al.</i> , | : | |
| | : | |
| Defendants. | : | |
| -----X | : | |

JAMES L. COTT, United States Magistrate Judge.

Defendants have requested that portions of the Court’s Opinion and Order dated August 18, 2021 be redacted. For the reasons explained below, the request is granted in part and denied in part.

I. BACKGROUND

On August 18, 2021, the Court issued its Opinion and Order on plaintiffs’ motion for sanctions temporarily under seal and directed the parties to advise the Court of any proposed redactions for the Court’s review. Dkt. No. 526 at 54. The Court reminded the parties to “be mindful of the presumption of public access to judicial documents in proposing any redactions.” *Id.* (citing *Brown v. Maxwell*, 929 F.3d 41, 47–48 (2d Cir. 2019) and *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 119–20 (2d Cir. 2006)). On August 23, 2021, defendants filed a letter with their proposed redactions, which they claim “relate exclusively to [d]efendants’ IT infrastructure.” Dkt. No. 527 at 1. In their letter, defendants request that the Court redact “information regarding [their] server locations, vendors, data storage

practices, and their use of specific hardware or software.” *Id.* Plaintiffs have not responded to defendants’ request.¹

II. DISCUSSION

A. Legal Standard

“There is a long-established ‘general presumption in favor of public access to judicial documents.’” *Beverly Hills Teddy Bear Co. v. Best Brands Consumer Prod., Inc.*, No. 19-CV-3766 (GHW), 2020 WL 7706741, at *2 (S.D.N.Y. Dec. 29, 2020) (quoting *Collado v. City of New York*, 193 F. Supp. 3d 286, 288 (S.D.N.Y. 2016)).

“The presumption of access is ‘based on the need for federal courts . . . to have a measure of accountability and for the public to have confidence in the administration of justice.’” *Id.* (quoting *United States v. Amodeo*, 71 F.3d 1044, 1048 (2d Cir. 1995)). Given this presumption, the Second Circuit has articulated a three-part test for evaluating whether documents (or certain information within those documents) may be sealed:

First, the court must determine whether the documents at issue are judicial documents. Second, it must assess the weight of the presumption of public access that attaches to those documents. Third, the court must ‘balance competing considerations against’ the

¹ As defendants note in their letter, an unredacted copy of the Opinion and Order is available via a link contained in an August 19, 2021 article appearing on Law 360. Dkt. No. 527 at 1, n.1. While the Court understands that the Opinion was briefly filed on the public docket in the morning on August 19 due to human error in the docketing process, it has not been able to determine why the version that appeared in the Law 360 article was different from the one originally filed on ECF. In any event, the fact that the Opinion apparently remains publicly available would appear to render this application academic. Nevertheless, because defendants, while acknowledging this fact, have still requested that the Court approve their proposed redactions – and because the issues presented in this application are somewhat novel – the Court is issuing this Memorandum Order.

presumption of access, such as ‘the danger of impairing law enforcement or judicial efficiency and the privacy interests of those resisting disclosure.’

Sylvania v. Ledvance LLC, No. 20-CV-9858 (RA), 2021 WL 412241, at *1 (S.D.N.Y. Feb. 5, 2021) (internal citations omitted) (quoting *Lugosch*, 435 F.3d at 120).

“[T]he proponent of sealing must ‘demonstrat[e] that closure is essential to preserve higher values and is narrowly tailored to serve that interest.’” *Bernstein v. Bernstein Litowitz Berger & Grossmann LLP*, 814 F.3d 132, 144 (2d Cir. 2016) (quoting *In re N.Y. Times Co.*, 828 F.2d 110, 116 (2d Cir. 1987)). “Broad and general findings’ and ‘conclusory assertion[s]’ are insufficient to justify deprivation of public access to the record; ‘specific, on-the-record findings’ are required.” *Id.* at 144–45 (internal citation omitted) (quoting *United States v. Erie Cnty.*, 763 F.3d 235, 243 (2d Cir. 2014)). Thus, “[t]o meet its heavy burden, the moving party ‘must offer specific facts demonstrating that closure is essential to preserve higher values and is narrowly tailored to serve that interest.’” *Beverly Hills Teddy Bear Co.*, 2020 WL 7706741, at *2 (quoting *Wells Fargo Bank, N.A. v. Wales LLC*, 993 F. Supp. 2d 409, 413 (S.D.N.Y. 2014)). “[T]he decision as to access [to judicial records] is one best left to the sound discretion of the trial court, a discretion to be exercised in light of the relevant facts and circumstances of the particular case.” *Id.* (quoting *Nixon v. Warner Commc’ns*, 435 U.S. 589, 599 (1978)).

B. Application

1. Judicial Documents

“A ‘judicial document’ or ‘judicial record’ is a filed item that is ‘relevant to the performance of the judicial function and useful in the judicial process.’” *Bernstein*, 814 F.3d at 139 (quoting *Lugosch*, 435 F.3d at 119). Because the information defendants wish to redact was submitted for the Court’s consideration in response to plaintiffs’ motion for sanctions and was related to the Court’s decision, the information is plainly included as part of judicial documents. *See, e.g., Valassis Commc’ns, Inc. v. News Corp.*, No. 17-CV-7378 (PKC), 2020 WL 2190708, at *2 (S.D.N.Y. May 5, 2020) (“[A]ll the documents at issue were submitted to the Court in support of and so would reasonably have the tendency to influence the Court’s decision on the outstanding motions . . . for sanctions. . . . As such, all documents submitted in support of these motions are judicial documents . . .”); *Capricorn Mgmt. Sys., Inc. v. Gov’t Emps. Ins. Co.*, No. 15-CV-2926 (DRH) (SIL), 2019 WL 5694256, at *22 (E.D.N.Y. July 22, 2019) (documents in support of Rule 37(e) sanctions motion are judicial documents), *adopted by* 2020 WL 1242616 (Mar. 16, 2020).

2. Weight of Presumption of Public Access

“The weight of the presumption is a function of (1) ‘the role of the material at issue in the exercise of Article III judicial power’ and (2) ‘the resultant value of such information to those monitoring the federal courts,’ balanced against ‘competing considerations’ such as ‘the privacy interests of those resisting disclosure.’”

Bernstein, 814 F.3d at 142 (quoting *Lugosch*, 435 F.3d at 119–20). “The presumption attached to . . . non-dispositive motions ‘is generally somewhat lower than the presumption applied to material introduced at trial, or in connection with dispositive motions such as motions for dismissal or summary judgment.’” *Valassis Commc’ns, Inc.*, 2020 WL 2190708, at *2 (quoting *Brown*, 929 F.3d at 50). Thus, the information defendants seek to redact is “subject to a lesser—but still substantial—presumption of public access.” *Id.* (quoting *Brown*, 929 F.3d at 53).

While the presumption of public access is lower given the non-dispositive nature of the motion at issue here, at least some of the information defendants seek to redact was used as part of the Court’s analysis and “the public would likely need access to the information . . . in order to understand the issues before the Court and evaluate the Court’s reasoning.” *Anderson v. New York City Health & Hosps. Corp.*, No. 16-CV-1051 (GBD) (KHP), 2020 WL 1047054, at *3 (S.D.N.Y. Mar. 4, 2020) (citing *Bernstein*, 814 F.3d at 141). For example, as discussed in more detail below, defendants seek to redact details regarding the inconsistencies in AMCI Holdings’ document preservation practice on page 12 of the Court’s Opinion and Order. However, this information was integral to the Court’s analysis in determining the extent of defendants’ dereliction of their duty to preserve ESI and whether email was actually lost. Accordingly, there is a strong presumption of public access to some of the information, at least to the extent the Court used it to shape and inform its analysis. *See, e.g., In re SunEdison, Inc. Sec. Litig.*, No. 16-CV-7917 (PKC), 2019 WL 12043498, at *2 (S.D.N.Y. Sept. 25, 2019) (“underlying materials [were]

afforded a high presumption of public access” because they were “an important part of defendants’ opposition . . . that was discussed in detail by the Court”); *Bernsten v. O’Reilly*, 307 F. Supp. 3d 161, 170 (S.D.N.Y. 2018) (“In order to evaluate that claim, the Court would need to review and analyze the [proposed redacted information]; thereafter, the public should be able to see what the Court relied on in issuing its Opinion. The public would have no way to make sense of the Court’s analysis testing this claim with only partial or limited access to the [proposed redacted information].”).

However, the inquiry does not end there. Rather, “[a]gainst the applicable presumption of public access,” the Court must next “consider whether countervailing factors or higher values dictate” redacting the proposed information. *Valassis Commc’ns, Inc.*, 2020 WL 2190708, at *1.

3. Competing Considerations

“Although the term [‘higher values’] has not been comprehensively defined, courts have identified particular examples of ‘higher values.’” *E.E.O.C. v. Kelley Drye & Warren LLP*, No. 10-CV-655 (LTS) (MHD), 2012 WL 691545, at *2 (S.D.N.Y. Mar. 2, 2012) (collecting cases). “Established factors and values that can outweigh the presumption of public access include legal privilege, business secrecy, and privacy interests.” *Echo Bay, LLC v. Torrent Pharma, Inc.*, No. 20-CV-6345 (PKC), 2020 WL 5543070, at *2 (S.D.N.Y. Sept. 16, 2020) (internal citations omitted).

Defendants argue that “information regarding server location, vendors, data storage practices, and use of specific hardware or software can be used to facilitate

unauthorized access, particularly where such information is gathered in a single source,” based on advice apparently provided to them from information security consultants, although they did not submit affidavits from their consultants detailing the extent of the harm or how the information could specifically be used by hackers.² They “further note that, ‘[c]ourts have concluded that concerns about hackers and a cyber attack justified sealing information about a company’s IT systems.’” Dkt. No. 527 at 1 (quoting *OneAmerica Fin. Partners, Inc. v. T-Sys. N. Am., Inc.*, No. 15-CV-1534, 2016 WL 891349, at *4 (S.D. Ind. Mar. 9, 2016)). The one case they quote from, in turn, cites three cases from the Northern District of California and a case from the Eastern District of Wisconsin, all of which found that concerns regarding cyber attacks could justify the sealing of certain information. For example, in *Music Group Macao Commercial Offshore Limited v. Foote*, the court described how certain categories of information can be used to “perpetuate a cyber attack including: (1) identification of a particular vulnerability in a company’s systems or software; (2) knowledge of the software or vendor of security software used; and (3) ‘social engineering’—*i.e.*, gaining the trust of a company insider to, in turn, gain access to the company’s software.” No. 14-CV-3078 (JSC), 2015 WL 3993147, at *5 (N.D. Cal. June 30, 2015). The court then reasoned that “[p]ublic

² It would have been preferable for defendants to have submitted affidavits from their consultants in support of their application. In the normal course, the Court would expect such evidence in support of the redactions that are being sought here. However, plaintiffs do not oppose defendants’ application, and the Court believes the record is sufficiently developed, especially given the expert reports submitted as part of the motion papers, to rule on defendants’ requests without further submissions.

release of this information could therefore cause [defendant] harm by contributing to [a] cyber attack.” *Id.*

Courts in the Second Circuit have not specifically addressed whether protecting a company from the threat of a “cyber attack” is a “higher value” or “countervailing factor” that can prevail over the presumption of public access.³ However, protecting a company’s IT information fits comfortably within other “higher values” consistently recognized by courts in this Circuit, such as the protection of “sensitive business information,” *Hanks v. Voya Ret. Ins. & Annuity Co.*, No. 16-CV-6399 (PKC), 2020 WL 5813448, at *2 (S.D.N.Y. Sept. 30, 2020) (collecting cases); the protection of “proprietary business information, such as internal analyses, business strategies, or customer negotiations,” *Sec. & Exch. Comm’n v. Telegram Grp. Inc.*, No. 19-CV-9439 (PKC), 2020 WL 3264264, at *3 (S.D.N.Y. June 17, 2020) (collecting cases); and “the prevention of potential fraud.” *Dollar Phone Corp. v. Dun & Bradstreet Corp.*, No. 09-CV-3645 (ILG) (SMG), 2012

³ The court in *Saint-Jean v. Emigrant Mortg. Co.* redacted information related to “cyber security and password setting,” but did not provide its reasoning for doing so. No. 11-CV-2122 (SJ) (RLM), 2016 WL 11430775, at *5 n.11 (E.D.N.Y. May 24, 2016). However, releasing documents related to a company’s “password setting,” would seem to be inherently riskier than making public, for example, the type of email defendants use. Regardless, if “password setting” and the types of information defendants seek to redact produce similar cybersecurity risks, defendants have not met their burden through “a particular and specific demonstration of fact.” *T-Jat Sys. 2006 Ltd. v. Amdocs Software Sys. Ltd.*, No. 13-CV-5356 (JMF), 2015 WL 394075, at *6 (S.D.N.Y. Jan. 29, 2015) (“[T]o justify sealing business information, a party must ‘make a particular and specific demonstration of fact showing that disclosure would result in an injury sufficiently serious to warrant protection; broad allegations of harm unsubstantiated by specific examples or articulated reasoning fail to satisfy the test.’” (quoting *Lytle v. JPMorgan Chase*, 810 F. Supp. 2d 616, 630 (S.D.N.Y. 2011))).

WL 13195012, at *2 (E.D.N.Y. May 10, 2012). *See also Kewazinga Corp. v. Microsoft Corp.*, No. 18-CV-4500 (GHW), 2021 WL 1222122, at *3 (S.D.N.Y. Mar. 31, 2021) (“Courts commonly find that documents that contain trade secrets, confidential research and development information, marketing plans, revenue information, pricing information, and the like satisfy the sealing standard.” (quoting *Rensselaer Polytechnic Inst. v. Amazon.com, Inc.*, No. 18-CV-549 (BKS) (CFH), 2019 WL 2918026, at *2 (N.D.N.Y. June 18, 2019))); *In re Am. Realty Cap. Properties, Inc. Litig.*, No. 15-CV-307 (AKH), 2019 WL 11863704, at *1 (S.D.N.Y. Mar. 25, 2019) (“Screenshots and any other information about . . . software that could be used to copy the program’s structure or functions are more deserving of protection . . .”).

In this vein, at least one court has grouped “IT information,” within the umbrella of “business information,” warranting redactions. *See Ramirez v. Temin & Co., Inc.*, No. 20-CV-6258 (ER), 2020 WL 6781222, at *6 (S.D.N.Y. Nov. 18, 2020) (“The Document also has several sections that include the Firm’s business information. Specifically, the categories of business information include: . . . IT information. The Court has established that business information constitutes confidential information . . . when it is ‘sufficiently valuable and secret to afford an actual or potential economic advantage over others.’” (internal citations omitted) (quoting *In re Parmalat Sec. Litig.*, 258 F.R.D. 236, 245 (S.D.N.Y. 2009))). Accordingly, the need to protect a party from a cyber security attack may be a legitimate basis to rebut the public’s presumption of access to judicial documents,

where the threat of a cyber security attack outweighs the extent to which the particular information was used to inform the Court’s opinion. With these principles in mind, the Court will now turn to defendants’ proposed redactions.

4. Categories of Redactions

Rather than going through each proposed redaction individually, the Court has grouped the redactions into the following eight categories: (1) the nature of defendant companies’ IT infrastructure (Dkt. No. 526 at 7); (2) the names of the companies that handle their IT and the employees affiliated with those companies (*id.* at 7, 8, 11 n.6, 14, 17, 40, 50, 51); (3) the providers of certain services related to email and document retention (*id.* at 7, 17, 30); (4) the location of a physical server (*id.* at 9, 12, 15, 20, 29); (5) descriptions of forensic digital files (*id.* at 8 n.4, 14 n.8, 15–21, 25, 26, 29, 31, 41, 49, 50); (6) Hans Mende’s, Fritz Kundrun’s, and Hans Fleskes’ specific preservation practices (*id.* at 9, 11, 18, 29, 30); (7) AMCI Holdings’ document retention policies (*id.* at 12, 16, 17, 40); and (8) details regarding specific document retention (*id.* at 18, 37). The specific information redacted within the first four categories was not required to shape the Court’s analysis and the public would not need access to this information to understand the Court’s Opinion. *See, e.g., Oliver Wyman, Inc. v. Eielson*, 282 F. Supp. 3d 684, 707 (S.D.N.Y. 2017) (“The remaining categories of information [plaintiff] hopes to seal all carry a low presumption of access to public records because they are collateral to the Court’s resolution of the parties’ . . . motions.”). The Court therefore grants defendants’

request to redact the information within those categories. The next four categories are more difficult to resolve. As such, the Court will discuss them in more detail.

First, defendants seek to redact descriptions of forensic digital files, which includes much of the information the Court examined in determining whether emails were permanently destroyed. For example, defendants seek to redact significant portions of the Court's descriptions of the parties' expert reports (Dkt. No. 526 at 16–20). The descriptions, if unsealed, would reveal the type of software defendants use to keep and store emails because they relate to the programs that defendants use for emails, which they contend “can be used to facilitate unauthorized access.” Dkt. No. 527 at 1. While defendants propose to redact much of the information in the description of the expert reports, they do not seek to redact similarly large portions of the Court's corresponding analysis. In particular, even with defendants' proposed redactions, the parts of the Court's Opinion and Order discussing whether the missing ESI could be restored through additional discovery remains largely intact. Dkt. No. 526 at 41–42. The presumption of public access is weaker then because the public would still be able to understand the Court's rationale for its decision without the specific details of defendants' email infrastructure. The Court therefore grants the redactions related to the descriptions of forensic digital files at Dkt. No. 526 at 8 n.4, 14 n.8, 15–21, 25, 26, 29, 31, 41, 49, 50.⁴

⁴ The Court notes that on page 20, on the sixth line of the last paragraph, defendants did not redact a phrase that was otherwise redacted throughout. That phrase should also be redacted to be consistent with the other redactions.

Next, defendants seek to redact information related to Hans Mende's, Fritz Kundrun's, and Hans Fleskes' specific preservation practices. While the specific preservation practices of Mende and Kundrun are crucial to the Court's analysis on defendants' duty to preserve ESI (Dkt. No. 526 at 37–38), defendants only seek to redact specific references related to IT practices.⁵ Defendants have thus narrowly tailored the proposed redactions without significantly affecting the public's access to understanding the Court's Opinion. The Court therefore grants the redactions related to Mende, Kundrun, and Fleskes' preservation practices at Dkt. No. 526 at 9, 11, 18, 29, 30.

Defendants also seek to redact information related to AMCI Holdings' document retention policies. Beginning at page 12 of the Court's Opinion and Order, defendants request that the specific references to the contradictions in AMCI Holdings' preservation practices and policies be redacted. On page 17, defendants similarly attempt to redact a comment that archiving at the AMCI Holdings office was done on an "ad hoc" basis. On pages 16 and 40, defendants wish to redact two sentences that refer to preservation practices and also detail how defendants' IT personnel archive information, both of which begin with the phrase "[defendants] archived emails 'at will.'" Many of these references lie at the heart of the Court's analysis in finding that sanctions were warranted because it was those inconsistencies that led the Court to its conclusions that AMCI Holdings failed to

⁵ Fleskes was not identified as a custodian in the case and the Court therefore did not discuss his ESI as part of its analysis on lost ESI when determining when defendants' duty to preserve ESI was triggered. Dkt. No. 526 at 10, 29.

take reasonable steps to preserve ESI and that ESI was ultimately lost. *See, e.g.*, Dkt. No. 526 at 40. Specifically, those references detail how defendants' counsel failed to "become fully familiar with [their] client's document retention policies, as well as the client[s'] data retention architecture." *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004). The presumption of public access is thus higher, and the threat of a cyber attack must be greater to justify redacting the information. *See, e.g., Anderson*, 2020 WL 1047054, at *3 ("[T]he public would likely need access to the information . . . in order to understand the issues before the Court and evaluate the Court's reasoning.").

Defendants have not met their burden to show that the threat of a cyber attack outweighs the public access to the following sentences on page 12: AMCI Holdings "does not have a written record retention policy;" it was AMCI Holdings' policy to "retain everything indefinitely;" it was "[t]he general practice of AMCI and AMCI Holdings . . . to delete, maintain and/or archive emails and documents at their discretion;" and AMCI Holdings "had no standard practice of preserving employee's emails."⁶ Defendants have not offered "a particular and specific demonstration of fact," *T-Jat Sys. 2006 Ltd.*, 2015 WL 394075, at *6 (quotation omitted), that this information can be used by hackers, nor is it apparent to the Court. The same applies to the Court's reference on page 17 that archiving at the AMCI Holdings office was done on an "ad hoc" basis. However, weighing the factors

⁶ References to the physical location of servers and employee names, as already discussed, can be redacted and were not included in the excerpts cited herein.

for the sentences on pages 16 and 40 produces a different conclusion. In particular, although the part of the sentences that mention that email archiving was done “at will” was important to the Court’s analysis, the rest of each sentence offers details regarding defendants’ IT practices, which are not as integral to the Court’s analysis, and potentially offer details that could be used maliciously by hackers. Accordingly, the Court will permit redaction of the latter half of each sentence (following the phrase “at will”) on pages 16 and 40.

Lastly, defendants seek to redact details regarding specific document retention at pages 18 and 37 of the Court’s Opinion and Order and references to “Tata Emails” on pages 16, 18, 36, 41, and 49. Both sentences refer to the fact that part of the missing emails were “archived on Defendants’ systems” that were recovered from a company called “Tata” in 2012. This fact was crucial to the Court’s determination that emails were lost after 2012, *i.e.*, after defendants’ duty to preserve ESI was triggered. Dkt. No. 526 at 36–37. Consequently, these references ultimately led to the Court’s conclusion that sanctions were warranted. Thus, there is far greater weight of a presumption of public access to these two sentences. Defendants have not provided “a particular and specific demonstration of fact,” that a hacker could use knowledge that email was archived in 2012 to infiltrate defendants’ current information systems. Defendants add that the threat of a cyber attack is greater where “information is gathered in a single source.” Dkt. No. 527 at 1. However, because the Court has granted the majority of defendants’ proposed redactions, the extent to which this particular information may be useful to a

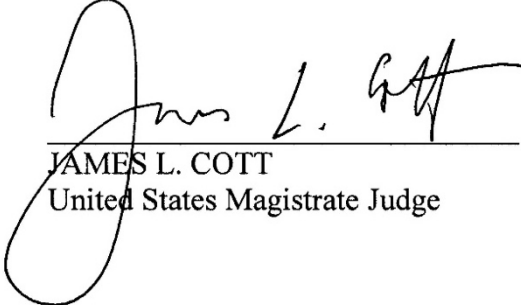
hacker, without the other information, is less likely. Accordingly, the Court denies the request to redact these two sentences as well as the Court's references to the "Tata Emails."

III. CONCLUSION

For the foregoing reasons, the Court grants defendants' requests for redactions except those at pages 12, 16, 17, 18, 36, 37, 40, 41, and 49, as discussed in this Memorandum Order. By September 15, 2021, defendants are directed to submit to the Court, by email, a redacted version of the Opinion and Order consistent with this Memorandum Order. The Court will, in turn, docket that version, and then submit it to Westlaw and Lexis for publication.

SO ORDERED.

Dated: September 10, 2021
New York, New York



JAMES L. COTT
United States Magistrate Judge